CLAIMS: The following is a listing of all claims in the application with their status and the text of all active claims

1. - 20. (CANCELED)

21. (CURRENTLY AMENDED) A method for delivering authentication authority Web services for user to use a single authentication device to generate non-reusable and non-reversible one-time identity codes, and subsequently use these codes to logon any computer on the Internet that he/she is authorized to access, the method comprising:

(a) registering user's public, private, and an authentication client device identities with an authentication authority;

(b) conducting synchronization between the authentication authority and the user's authentication client device;

(c) generating an one-time identity code from the authentication client device before each logon event for authentication;

(d) submitting the one-time identity code to a business application server;

(e) composing an user identity verification request message by an authentication handler which is a plug-in software installed on the business application server;

(f) submitting the identity verification request message by the authentication handler to an authentication gateway authority using Web services method;

(g) forwarding the identity verification request message from the gateway authority to the authentication authority;

(h) verifying the user's identity by the authentication authority by checking the one-time identity code included as a part of the identity verification request message;

(i) composing an identity verification response message and sending the authentication handler the response message by the authentication authority;

(j) receiving the identity verification response message by the authentication handler;

(k) informing the business application server about the verification status by the authentication handler;

(l) granting permission for the user to access protected resources by the business application server upon a positive user identity verification.

22. (PREVIOUSLY PRESENTED) The method of claim 21, further comprising: establishing and publishing the authentication authority Web services to Web service industry's registries by the authentication authority.

23. (PREVIOUSLY PRESENTED) The method claim 22 wherein establishing and publishing the authentication authority Web services by the authentication authority, comprises: using Web Services Description Language (WSDL) to publish the authentication authority Web services, and using Universal Description, Discovery and Integration (UDDI) standard to discover the authentication authority Web services published by other authorities.

24. (PREVIOUSLY PRESENTED) The method of claim 21, wherein the gateway authority and the authentication authority to be separated and placed in the Internet accessible environment to achieve a scalable and distributable solution.

25. (PREVIOUSLY PRESENTED) The method of claim 21, wherein the authentication authority and the authentication client device contain means to generate one-time and non-predictable identity codes independently for user identity authentication or verification.

26. (PREVIOUSLY PRESENTED) The method of claim 21, wherein the synchronization is conducted by executing a set of math function comprising hash, power and modular math operators with the input of information comprising user public identity, authentication client device identity, and user private identity.

27. (PREVIOUSLY PRESENTED) The method of claim 21, wherein the authentication authority and the authentication client device contain means to generate confirmation codes to verify the success of the synchronization.

28. (CURRENTLY AMENDED) The method of 26, wherein the user private identity comprises the user's biometric identity and other shared secret information which doesn't have risk of being exposed over the Internet.

29. (CURRENTLY AMENDED) The method of claim 21, wherein the authentication client device comprising the use of portable, hand-held devices to generate one-time and non-predictable identity codes locally and independently.

30. (CURRENTLY AMENDED) The method of claim 21, wherein the method can be used as an ID verification method for any business entity to verify the user identity using one-time and non-predictable identity codes over a channel selected from the group consisting of the Internet, phone and other communication means.

31. (CURRENTLY AMENDED) A system for delivering authentication authority Web services for user to use a single authentication device to generate non-reusable and non-reversible one-time identity codes, and subsequently use these codes to logon any computer on the Internet that he/she is authorized to access, the system comprising:

a. means for registering user's public, ~~and~~ private, and an authentication client device identities with an authentication authority;
b. means for conducting synchronization between the authentication authority and the user's authentication client device;
c. means for generating an one-time identity code from the authentication client device before each logon event for authentication;
d. means for submitting the one-time identity code to a business application server;

e. means for composing an user identity verification request message by an authentication handler which is a plug-in software installed on the business application server;

f. means for submitting the identity verification request message by the authentication handler to an authentication gateway authority using Web services method;

g. means for forwarding the identity verification request message from the gateway authority to the authentication authority;

h. means for verifying the user's identity by the authentication authority by checking the one-time identity code included as a part of the identity verification request message;

i. means for composing an identity verification response message and sending the authentication handler the response message by the authentication authority;

j. means for receiving the identity verification response message by the authentication handler;

k. means for informing the business application server about the verification status by the authentication handler;

l. means for granting permission for the user to access protected resources by the business application server upon a positive user identity verification.

32. (PREVIOUSLY PRESENTED) The system of claim 31, further comprising: means of establishing and publishing, by the authentication authority, the authentication authority Web services to Web service industry's registries.

33. (PREVIOUSLY PRESENTED) The system of claim 31, wherein the gateway authority and the authentication authority contain means to be separated and placed in the Internet accessible environment to achieve a scalable and distributable solution.

34. (PREVIOUSLY PRESENTED) The system of claim 31, wherein the authentication authority and the authentication client device contain means to generate one-time and non-predictable identity codes independently for user identity authentication or verification.

35. (PREVIOUSLY PRESENTED) The system of claim 31, wherein the synchronization is conducted by executing a set of math function comprising hash, power and modular math operators with the input of information comprising user public identity, authentication client device identity, and user private identity.

36. (PREVIOUSLY PRESENTED) The system of claim 31, wherein the authentication authority and the authentication client device contain means to generate confirmation codes to verify the success of the synchronization.

37. (CURRENTLY AMENDED) The system of claim31, wherein the authentication client device comprising the use of portable, hand-held devices to generate one-time and non-predictable identity codes locally and independently..

38. (PREVIOUSLY PRESENTED) The system of claim 31, wherein the gateway authority, the authentication authority, the authentication handler, and the authentication client device are arranged to use Simple Object Access Protocol (SOAP) to communicate, and use Hypertext Transport Protocol (HTTP) packets to transmit data over Secure Socket Layer (SSL).

39. (CURRENTLY AMENDED) The system of claim 31, wherein the system can be used as an ID verification system for any business entity to verify the user identity using one-time and non-predictable identity codes over a channel selected from the group consisting of the Internet, phone and other communication means.